PCT/IB 04/2345

Europäisches Patentamt | European Patent Office | Office européen des brevets

PCT/IB04/2345

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

03291823.7

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

REC'D 04 AUG 2004
WIPO PCT

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03291823.7
Demande no:

Anmeldetag:
Date of filing: 23.07.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

SCHLUMBERGER Systèmes
50, avenue Jean Jaurès
92120 Montrouge
FRANCE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Procedure for monitoring the usage of a broadcasted content

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04N7/16

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR LI

Procedure for monitoring the usage of a broadcasted content

Description

1 What is the field of the invention?

The invention describes mechanisms to enable an accurate monitoring of the services used by a subscriber of a broadcast service.

The invention relates to services that are broadcasted through a wired/wireless network encrypted with keys that are managed inside a tamper resistant device as the smartcard.

2 What is already known?

-A broadcast service corresponds to a specific data flow that is broadcasted through a network. To enable that only subscribed users may access to a specific service, this data flow may be encrypted with an encryption key (EK) that is given through different mechanisms to users that are subscribed to this particular service.

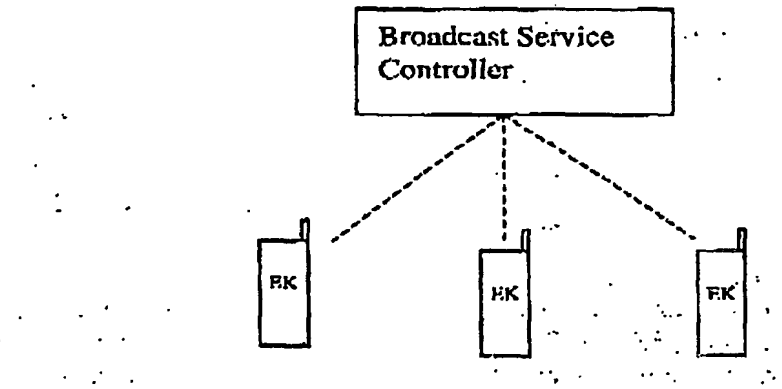


FIG 1

-To avoid that unsubscribed users may access to the EK and so be able to use the service for free. this EK is usually renewed frequently. One of the mechanisms of this renewal of keys that is currently used consists on the following components:

-a smart card (or any other hardware protected and tamper resistant device) is provided to the subscribers accessing a particular service. This smartcard is provisioned with a key encryption key (KEK), which is the same for all subscribers accessing this particular service. This KEK may also be updated by means of different mechanisms. One needed characteristic of this KEK is that it is never revealed in clear outside the smartcard. Whether it needs (for managing purposes, for instance) to be handed through unsafe network entities (e.g. the terminals) this is also encrypted. The KEK is identified by a KEK identifier (KEK_ID), associated to a particular broadcasted service.

-The data flow is broadcasted encrypted with the EK. The data flow contains regularly some data, Management Container (MC), which is used for key management and eventually for other purposes. This MC may contain:

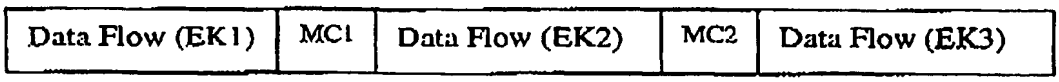
- The identifier of the KEK (KEK_ID) that is being used in the current broadcasted service.
- An encrypted encryption key (EEK), that corresponds to the EK being used in the current data flow encrypted with the KEK corresponding to the KEK_ID being sent.
- Other additional data that will be further considered in this document.

-A terminal that is responsible to listen the data flow corresponding to the broadcasted service. The terminal is also responsible for decrypting the data flow using the valid EK.

-To obtain the valid EK the terminal regularly receives the MC and retrieves the KEK_ID and the EEK. Further, it sends this information to the smartcard, asking it to decrypt this EEK to obtain the corresponding EK. This decryption is performed using the KEK (stored in the smartcard) that corresponds to the KEK_ID being used. If the KEK_ID is known by the smartcard, it can then decrypt the EEK and send the EK back to the terminal. In this way, the terminal can continue to decrypt the data flow.

-As it is shown in the figure 2, the broadcast service provider is able to dynamically change regularly the EK, just by sending a new EEK in a previous MC message.

Broadcast Data Flow:



Note : FIG 2

Data Flow (EK1) : Data Flow associated with a particular service encrypted with EK1
MC1 : Management container including a new EEK2 asociated with a new EK2.
MC2 : Management container including a new EEK3 asociated with a new EK3.

3 What problem needs to be solved?

The explained model is well adapted to provide a frequent renewal of keys based in the above broadcast principles. In this model, a particular user does not need to contact the service provider every time that new encryption keys are needed to decrypt the content. It just need to obtain the EEK listening to the broadcasted data flow and ask locally the smartcard to retrieve the EK needed.

However, there is a main limitation in this model: the service provider, or any other network entity responsible for control or charging of a particular broadcast service, hereafter referred as service controller (SC), is not able to know whether the user has effectively used this particular service.

As the renewal of keys is performed locally, the SC is not able to know whether the user has effectively used the broadcast content, as it is not aware if the broadcasted EEK has being used by the terminal or not. This is a big problem for services that are charged by the amount of data being used (time or volume charging).

Requiring the terminal to send back parameters describing the time (or the volume of data) that the user has been using a particular broadcast service could solve this difficulty. However, in order to disturb or cancel this control policy, the terminal is highly suitable to be attacked by the user. It means that, in this context, the terminal cannot be trusted to be involved in any monitoring of data that is used in the charging infrastructure.

4 How is the problem solved?

The solution proposed consists in the following new elements.

-The smartcard is provided with one or more counters associated to a particular broadcast service (and so, to a particular KEK). These counters are referred hereafter as encryption key counters (EKC).

Additionally the smartcard is provided with at least three fields for each of the broadcast services: Current EEK (CEEK) and current EK (CEK) and one or more maximum EKC value (MEKC) (one for each EKC).

-The following procedures are applied (see fig 3 and 4):

-Every time the terminal needs to renew the EK (associated with the reception of a MC message) it sends a PROVIDE-EK command to the smartcard. This command contains at least the broadcasted values KEK_ID and the EEK.
-The smartcard receives this values and performs the following tasks:

A) It searches if the KEK_ID exist (meaning that the using is subscribed to this particular broadcast service). If it does not, it refuses further processing of the command, sending a corresponding error message to the terminal. If it exist it continues the execution.
B) It tests whether the EEK correspond to the stored CEEK. If it does, it sends back the stored CEK. Else, It continues the execution.
C) If each of the EKC is smaller than the MEKC associated, it adds one to the EKC values and continue in step D. Else, it stops the execution, sending a corresponding error message to the terminal.
D) It uses the content of the KEK associated with the KEK_ID to decrypt the EEK obtaining the new EK to be used by the terminal. Further it stores this values in CEEK and CEK. Then it sends back the current EK to the terminal.

-Additionally an MC may contain additional management data (AMD) containing (see fig 5):

-A command header defining at least one of the following functions:
A-Change KEK
B-Reset/Update counter
C-Retrieve Subscription data. (e.g. EKC)

-At least the following command parameters depending on the command header:

A-KEK_ID and New KEK value
B- KEK_ID ,counter number, reset value
C- KEK_ID

-This AMD is encrypted with an upper level key, management key (MK) that can be provisioned in each of the smartcards.

-When receiving a MC that contains an encrypted AMD, the terminal, will pass it to the card through the MANAGEMENT_OPERATION command. The card will perform the corresponding actions and will send back to the terminal the corresponding results/response data encrypted and integrity protected with the same MK. The terminal will be responsible to send back this information to the SC through a known protocol based in a point-to-point mechanism.

Additionally, the same procedure may be defined if the AMD is not broadcasted in the Data flow but sent directly to the terminal in a point-to-point schema.

-The main advantage of this approach is that it is resistant to attacks in the terminal:

A-Some AMD are needed to perform some required operations to enable the subscriber continue receiving the Broadcast service (e.g. modify KEK_ID)

B-Further, From the terminal/user perspective is it impossible to know which is the nature of the command/results being sent to/from the smartcard.

As a consequence from A and B, the terminal cannot be modified/hacked in order to tamper/avoid the correct commands that are responsible of the subscriber charging, without consequences in the subscriber's service. (denial of service).

5 Detailed description of a practical example

A Mobile Network Operator (MNO) offers to its subscribers the possibility to subscribe to one Multimedia Broadcast Service (MBS). All MNO's subscribers have a terminal that may listen the broadcasted data. However only the subscribers of the Broadcast service are provided with the following mechanisms in its USIM (Universal subscriber identity module):

-A KEK_ID corresponding to this Service
-Two counters EKC1, EKC2
-One MEKC2
-A MK that may be associated with different services.

The service is provided following some principles:

-The KEK is usually changed once per month.
-The subscribers are charged each month by the amount of time that have been accessing the service.
-For parental control restrictions policy, some subscribers are limited to a certain amount of time each day. The MECK2 is then provisioned to a certain value.

The EK is changed regularly (each minute). Additionally, MC message are broadcasted more often, even with the same KEK-ID and EEK pairs (With or without AMD). When the subscriber is using the service, a PROVIDE-EK command with a new EK is then performed on the average of once a minute.

The following communications related to this particular MBS are held between the terminal and the MNO in a point-to-point base:

-Once a day each terminal/USIM receives an AMD containing a Reset/Update counter request with the value cero to the MECK2 counter. The MNO receives a confirmation of the result of this operation.

-At least once a month, the terminal/USIM receives and AMD containing a Retrieve Subscription data command. The command result is send back to the MNO. This is used by the MNO to generate the corresponding charging records by using the EKC1 counter value.
-For security reasons the KEK is usually changed at least once per month by receiving the terminal/USIM the Change KEK command.

Additionally different services may be provided with different KEK_ID. The different combinations of EK change, EKC and MEKC provide the necessary flexibility in the charging and monitoring of the service being used.

Claim

1. Method for monitoring the usage of services that are broadcasted through a wired/wireless network encrypted with keys that are managed inside a tamper resistant device in particular a smartcard, characterized in that the smartcard is provided with one or more counters associated to a particular broadcast service.

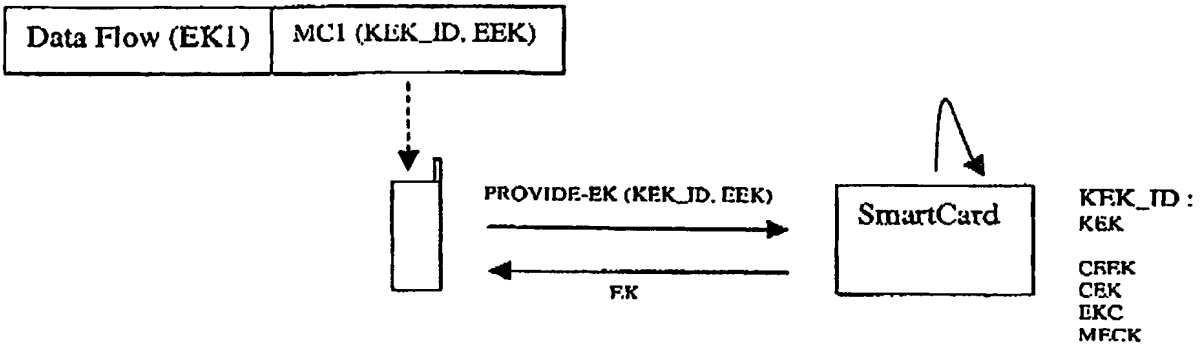

Data Flow (EK1)
MC1 (KEK_ID, EEK)
PROVIDE-EK (KEK_ID, EEK)
EK
SmartCard
KEK_ID :
KEK
CREK
CEK
EKC
MEKC

FIG 3

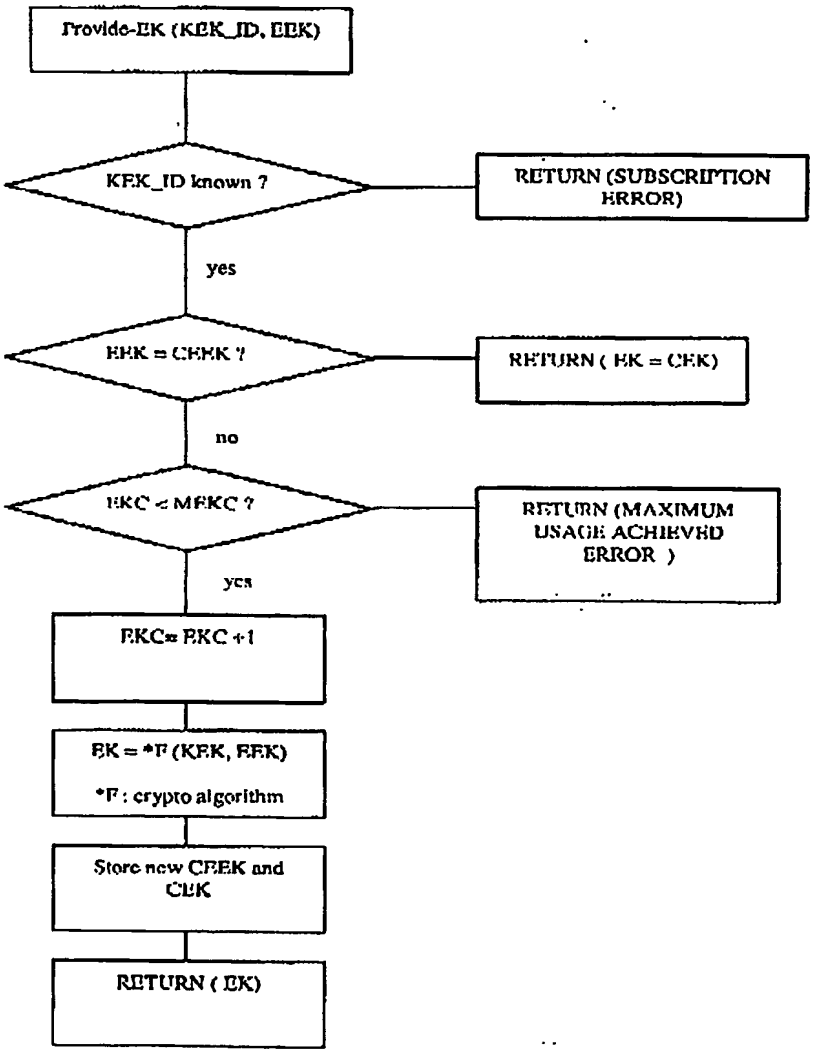

Provide-EK (KEK_ID, EEK)
KEK_ID known ?
RETURN (SUBSCRIPTION ERROR)
yes
EEK = CEEK ?
RETURN (EK = CEK)
no
EKC < MEKC ?
RETURN (MAXIMUM USAGE ACHIEVED ERROR)
yes
EKC= EKC +1
EK = *F (KEK, EEK)
*F : crypto algorithm
Store new CREK and CEK
RETURN (EK)

FIG 4

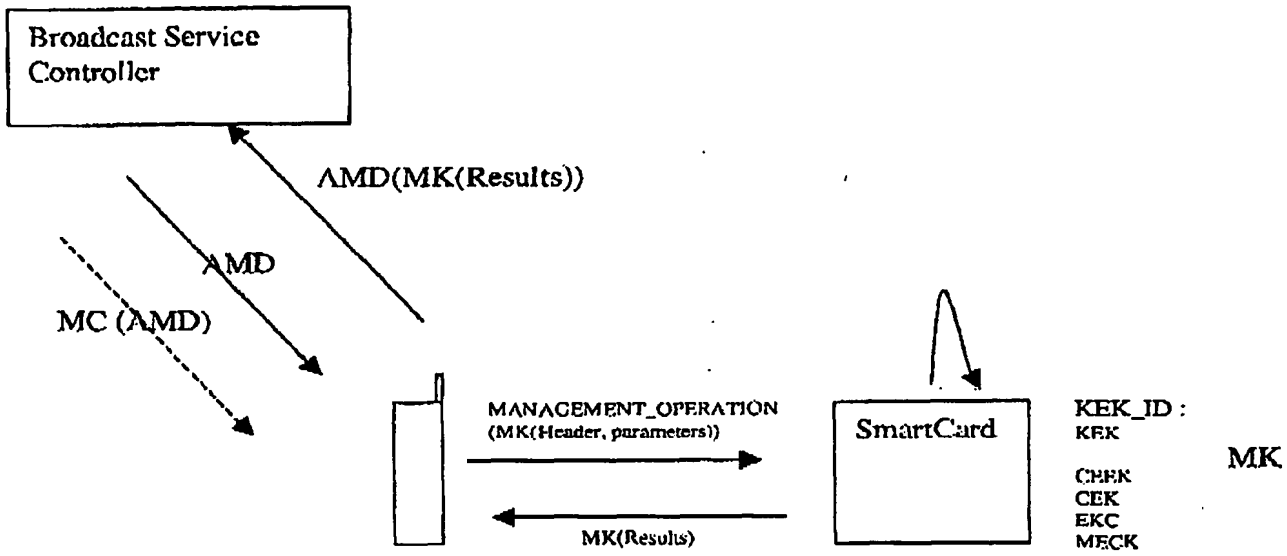

Broadcast Service Controller
AMD(MK(Results))
AMD
MC (AMD)
MANAGEMENT_OPERATION
(MK(Header, parameters))
MK(Results)
SmartCard
KEK_ID :
KEK
CHEK
CEK
EKC
MECK
MK

FIG 5